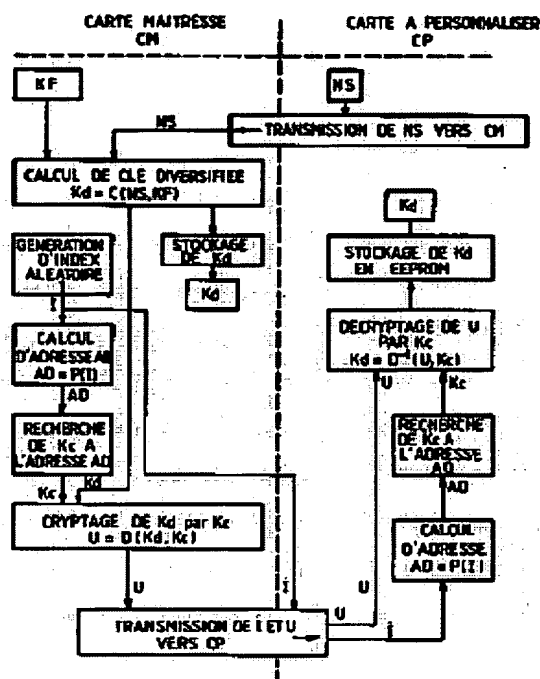


Process for transmitting confidential information between two chip cards

Patent number: FR2681165
Publication date: 1993-03-12
Inventor: AUGUSTIN FARRUGIA
Applicant: GEMPLUS CARD INT (FR)
Classification:
 - international: G06F12/14; G06K19/07; G06K19/073; G09C1/00
 - european: G07F7/10E, H04L9/08, G07F7/10D2, G07F7/10D4E2, G07F7/10D16
Application number: FR19910011009 19910905
Priority number(s): FR19910011009 19910905

Abstract of FR2681165

The invention relates to the encrypted transmission of information (K_d) between two microprocessor cards (CM, CP). The information is encrypted in the first card, the encrypted information is transmitted from the first card to the second, and the information is decrypted in the second card. The feature of the invention is that use is made of an encryption key drawn from a store of potential keys which consists of the read-only memory (120 for CM, 220 for CP) of the card. An index, generated by the first card and transmitted to the second card, is used so that the two cards may use the same key without transferring this key in clear between the two cards. The key is the contents of the read-only memory file at the address defined by the index. Application to the transmission of a secret key (K_d), diversified from a base key (K_F), between a diversification card (CM) and a card to be personalised (CP).



Data supplied from the esp@cenet database - Worldwide

PARIS

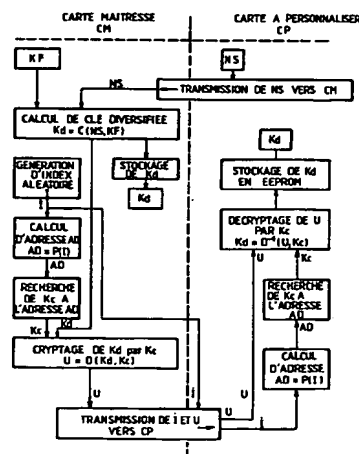
(51) Int Cl⁵ : G 06 K 19/07, 19/073; G 06 F 12/14; G 09 C 1/00

91 11009

A1

(74) Mandataire : Cabinet Ballot-Schmit.

Application à la transmission d'une clé secrète (Kd), diversifiée à partir d'une clé de base (KF), entre une carte de diversification (CM) et une carte à personnaliser (CP).



FR 2 681 165 - A1



PROCEDE DE TRANSMISSION D'INFORMATION CONFIDENTIELLE
ENTRE DEUX CARTES A PUCES

L'invention concerne la sécurité dans les applications des cartes à puces. Plus précisément elle concerne la transmission sécurisée d'informations entre deux cartes à puces.

5 On décrira l'invention à propos d'un cas particulier, bien que l'invention ait des applications plus générales. Ce cas particulier est celui de l'élaboration de clés de cryptage secrètes, diversifiées à partir d'une clé de base, qui doivent être placées
10 dans des cartes à puces qu'on veut utiliser dans une application déterminée.

Pour une application déterminée, application bancaire par exemple, l'émetteur de cartes à puces (la banque par exemple) va distribuer une carte à chaque
15 client. Cette carte devra comporter dans sa mémoire interne une clé de cryptage secrète, non connue et non accessible même par le titulaire de la carte. Cette clé servira à crypter la transmission d'informations entre la carte et l'appareil de transaction qui va utiliser la
20 carte. L'appareil de transaction connaîtra la clé secrète, pour pouvoir décrypter la transmission.

La clé secrète sera différente pour chaque carte, et c'est pourquoi elle est appelée clé diversifiée.

Il est donc nécessaire, à un certain stade de
25 l'élaboration des cartes, de placer une même clé secrète à la fois dans la carte d'un titulaire et dans l'appareil de transaction (ou dans le système informatique général qui pilote les appareils de transaction). Il y a donc nécessité de transmettre une
30 information confidentielle d'un organe à un autre.

Cette opération est délicate car il y a un risque qu'une personne chargée de ce travail et pouvant donc avoir de ce fait accès aux clés secrètes, ne s'en serve pour réaliser frauduleusement des cartes ayant toutes
5 les capacités des cartes légitimes.

Evidemment on peut crypter à nouveau la transmission de l'information confidentielle. Mais pour cela il faut une clé de cryptage et cette clé doit aussi être transmise. On n'a fait que reporter le problème.

10 Par exemple, une technique de production d'une clé diversifiée pour une application à utilisateurs multiples est la suivante : on utilise deux cartes à puces semblables, dont l'une est une carte maîtresse chargée d'élaborer et éventuellement de garder en
15 mémoire la clé diversifiée, et l'autre est une carte esclave ou carte à personnaliser, devant recevoir dans sa mémoire la clé secrète diversifiée qu'elle devra utiliser par la suite pour des opérations d'authentification. La carte maîtresse pourra servir à
20 transporter, vers les appareils de transaction ou vers le système qui les gère, la liste des clés diversifiées autorisées.

Dans cette technique, la carte maîtresse contient un microprocesseur avec une mémoire de programmes, et
25 dans cette mémoire un programme d'élaboration de clé diversifiée. Mais comme la clé diversifiée ne doit pas circuler en clair entre les deux cartes (pour éviter les fraudes), la carte comprend aussi un programme de cryptage pour envoyer la clé diversifiée sous une forme
30 indéchiffrable. La clé diversifiée est donc calculée, puis cryptée; le résultat du cryptage est envoyé à la carte à personnaliser.

La carte à personnaliser contient aussi un microprocesseur et une mémoire de programmes, et dans

cette mémoire un programme de décryptage permettant de retrouver la clé diversifiée à partir du signal crypté qu'elle reçoit.

5 Le programme de cryptage utilise une clé secrète de cryptage qui, bien entendu, doit rester confidentielle, faute de quoi une reconstitution de clés diversifiées serait possible, entraînant le risque de production frauduleuse de cartes.

10 Mais le programme de décryptage doit connaître cette clé, faute de quoi il ne pourrait pas reconstituer la clé diversifiée qu'il attend. Il faut donc que la carte à personnaliser contienne, dans une zone de mémoire inaccessible, cette même clé de cryptage. Et par conséquent il faut qu'à un moment ou un autre du procédé
15 de cryptage on place dans les deux cartes à la fois une même clé de cryptage, qui ne sert que provisoirement pour envoyer de la carte maîtresse vers la carte à personnaliser la clé diversifiée.

20 Il y a donc un risque qu'une personne mal intentionnée utilise la connaissance qu'elle a de cette clé pour reconstituer à des fins frauduleuses tout le processus de fabrication d'une clé diversifiée. Cette personne pourrait alors réaliser de fausses "vraies cartes".

25 Le but de l'invention est d'éviter ce risque par un moyen relativement simple.

Selon l'invention, on utilise le fait que la carte maîtresse et la carte à personnaliser ont dans leur mémoire morte des programmes ou des portions de
30 programmes identiques, ne serait-ce que parce qu'elles sont faites par le même fabricant, ou parce qu'elles ont un système d'exploitation identique ou parce qu'elles respectent des critères de normalisation identiques. Dans la pratique, la mémoire morte des deux cartes sera

même rigoureusement identique.

L'idée maîtresse de l'invention est d'utiliser comme clé de cryptage commune aux deux cartes une donnée prise parmi un fichier (et de préférence le fichier de
5 mémoire morte du système d'exploitation de la carte) dont le contenu et l'organisation sont identiques dans les deux cartes, la donnée étant désignée à partir d'un index transmis d'une carte à l'autre et susceptible de varier.

10 Par conséquent, au lieu d'avoir à inscrire dans deux cartes différentes une clé de cryptage commune avec le risque que cette inscription double permette ensuite une fraude, on utilise comme clé de cryptage un contenu déjà inscrit mais inconnu a priori et pouvant varier
15 d'une opération à une autre. Si de plus l'adresse à laquelle on va chercher ce contenu varie de manière aléatoire, on aboutit à une très grande sécurité.

Selon un aspect de l'invention, on propose donc un procédé de transmission cryptée d'une information entre
20 deux cartes à microprocesseur qui ont chacune un fichier de mémoire à plusieurs adresses, ce fichier ayant un contenu identique pour les deux cartes, procédé dans lequel on crypte l'information dans la première carte, on transmet l'information cryptée de la première carte à
25 la deuxième, et on décrypte l'information dans la deuxième carte, ce procédé étant caractérisé en ce que le cryptage et le décryptage sont effectués avec pour clé le contenu d'une partie seulement du fichier de mémoire, identifiée par une donnée d'adressage qui est
30 utilisée par la première carte et transmise à la deuxième carte.

La donnée d'adressage peut être une adresse proprement dite, mais de préférence elle sera plutôt un index à partir duquel on peut calculer une adresse. Les

deux cartes possèdent alors en mémoire le même programme de calcul d'une adresse à partir d'une valeur d'index.

Selon un aspect important de l'invention, c'est la mémoire morte de la carte, celle qui contient le système d'exploitation de la carte qui va être utilisée. Elle constitue en effet un fichier dans lequel on peut puiser un grand nombre de clés (chaque clé correspondant par exemple à un mot ou plusieurs mots consécutifs de mémoire).

L'invention est applicable notamment mais non exclusivement au cas évoqué dans le préambule, à savoir le cas où l'information à transmettre de manière cryptée entre les deux cartes est elle-même une clé de cryptage; et notamment lorsque cette information est une clé diversifiée qui doit être calculée par la première carte et stockée de manière confidentielle dans la deuxième.

Une manière de mettre en oeuvre l'invention consiste à utiliser, pour chaque opération de transmission cryptée entre les deux cartes, un générateur de donnée aléatoire interne à l'une des cartes (de préférence la première); ce générateur fournira une donnée non prévisible pouvant servir d'index pour le calcul d'une adresse de mémoire de chaque carte. Cet index aléatoire permettra de définir une clé de cryptage; il sera utilisé par la première carte pour crypter la transmission, et il sera envoyé à la deuxième carte en même temps que l'information cryptée pour permettre le décryptage. Lors d'une nouvelle opération, le générateur aléatoire fournira une autre adresse de mémoire.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description détaillée qui suit et qui est faite en référence aux dessins annexés dans lesquels :

6

- la figure 1 représente un système de diversification de clé dans lequel la présente invention peut être mise en oeuvre;

- la figure 2 représente schématiquement les deux
5 cartes du système;

- la figure 3 représente les étapes principales du procédé de transmission sécurisée de l'invention.

L'invention est applicable de manière générale à la transmission d'information cryptée entre deux cartes
10 ayant chacune au moins une mémoire figée dont le contenu est commun aux deux cartes; la description qui suit sera donnée en référence à l'exemple particulier de la transmission d'une clé diversifiée entre une carte maîtresse et une carte à personnaliser avec une clé
15 diversifiée.

A la figure 1 on a donc représenté un système capable de recevoir deux cartes et de permettre un dialogue entre les deux cartes. Le système peut être un microordinateur à usage général PC avec un clavier CL,
20 un écran SC et deux lecteurs de cartes LC1 et LC2, ou bien ce peut être un système spécialement conçu pour l'opération de diversification. Il doit pouvoir réaliser la transmission d'informations entre deux cartes à puces.

25 L'une des cartes est la carte maîtresse CM; l'autre est la carte à personnaliser CP.

Les deux cartes sont des cartes à microprocesseur, comportant un microprocesseur, une mémoire vive de travail (RAM), une mémoire morte de programmes (ROM)
30 contenant au moins le système d'exploitation de la carte, et une mémoire non volatile électriquement inscriptible (EPROM ou EEPROM ou Flash EPROM). Cette dernière mémoire contient en principe des programmes d'application, mais elle peut contenir aussi d'autres

données, et notamment des numéros d'identification, et la clé secrète diversifiée qu'on va chercher à y mettre.

Classiquement, certaines zones de la mémoire non volatile inscriptible électriquement sont non
5 accessibles en lecture et en écriture, sauf par le microprocesseur dans certains programmes du système d'exploitation.

Le contenu de la mémoire morte de programmes n'est d'ailleurs pas accessible sur les bornes extérieures de
10 la carte. Seul le microprocesseur peut aller le chercher, uniquement lors de certains programmes du système d'exploitation.

Sur la figure 2 on a représenté les deux cartes sous forme schématique, avec leur microprocesseurs (MP1
15 pour la carte maîtresse, MP2 pour la carte à personnaliser), leur mémoire vive (110, 210) leur mémoire morte (120, 220) leur mémoire non volatile (130, 230), et un interface de communication avec l'extérieur (140, 240).

20 L'élaboration de la clé diversifiée, à placer à la fois dans la mémoire non volatile de la carte à personnaliser et dans la mémoire non volatile de la carte maîtresse, se fait comme suit :

Une donnée NS est envoyée par la carte à
25 personnaliser CP à la carte maîtresse CM. Cette donnée peut être le numéro de série de la carte, inscrit dans sa mémoire non volatile 230.

Cette donnée sert à l'élaboration de la clé diversifiée Kd qu'on veut élaborer.

30 Par exemple, la valeur Kd est élaborée à partir de NS par une fonction de cryptage à clé secrète $C(NS, KF)$ où KF est une clé secrète contenue dans la carte maîtresse. Le programme de calcul de cette fonction est contenu dans la mémoire de la carte MP et est exécuté

par le microprocesseur de cette carte. La fonction $C()$ est de préférence l'algorithme standard DES ("Data Encryption Standard") publié par le National Bureau of Standards des USA, dans Federal Register vol 40, N°52 du 5 17 Mars 1975 et N° 149 du 1er Août 1975.

La clé diversifiée K_d à mettre dans la carte à personnaliser est donc $K_d = C(NS, KF)$. Elle est destinée à être transmise à la carte à personnaliser, mais par ailleurs elle peut être enregistrée dans la carte 10 maîtresse, ou être envoyée par tout moyen à l'application dans laquelle la carte sera utilisée. La carte maîtresse peut elle-même servir de vecteur de transmission vers un ordinateur central de cette application.

15 Dans certains cas, il n'est même pas nécessaire de conserver la clé K_d autrement que dans la carte à personnaliser. C'est le cas lorsque l'application ne cherche pas à vérifier précisément chaque clé diversifiée mais cherche tout simplement à vérifier si 20 la clé présente dans la carte est bien une clé diversifiée à partir d'une clé de base KF déterminée.

Pour ne pas transmettre en clair la clé K_d à la carte à personnaliser on procède de la manière indiquée ci-après.

25 Un index I de valeur aléatoire, non répétitive d'une étape de diversification de clé à une autre est élaboré.

Sommairement, on peut créer cet index à partir d'un générateur pseudo-aléatoire physique, ou avec un 30 programme contenu dans la mémoire de la carte maîtresse; ce programme peut utiliser le contenu d'un registre non volatile incrémenté à chaque nouvelle opération et une fonction de cryptage telle que l'algorithme DES, éventuellement avec la même clé secrète KF déjà utilisée

précédemment ou avec n'importe quelle autre clé. Le nombre ainsi généré peut être considéré comme aléatoire et non répétitif pour les besoins pratiques.

L'index de valeur aléatoire I va servir à calculer
5 une adresse de mémoire morte. Pour augmenter la sécurité, on préfère ne pas utiliser directement l'index comme adresse ou comme saut d'adresse. Mais on effectue un calcul, par exemple une fonction polynomiale, pour générer une adresse $AD = P(I)$. On s'arrange pour que
10 cette adresse reste contenue dans des limites telles que n'importe quelle adresse ainsi générée désigne un mot de mémoire d'un fichier identique dans les deux cartes.

Le programme de calcul de l'adresse AD à partir de I est contenu dans une mémoire de la carte maîtresse,
15 mais aussi dans une mémoire de la carte à personnaliser.

L'index I sera transmis en clair à la carte à personnaliser.

L'adresse AD est utilisée par le microprocesseur qui va lire dans la mémoire de la carte, à l'adresse AD,
20 un contenu qui sera considéré comme une clé de cryptage Kc pour une fonction de cryptage $D(Kd, Kc)$ de la clé de diversification Kd.

Le fichier choisi pour servir ainsi de réserve de clés de cryptage est le fichier de mémoire morte, celui
25 qui contient le système d'exploitation de la mémoire, car d'une part il est identique pour les deux cartes, et d'autre part il contient suffisamment de mots pour constituer une réserve de nombreuses clés de cryptage possibles.

30 Le programme de cryptage $D()$ qui va utiliser la clé trouvée à l'adresse AD est contenu dans la mémoire de la carte maîtresse; il est exécuté et le résultat $D(Kd, Kc)$ est transmis à la carte à personnaliser en même temps que l'index I.

10

La carte à personnaliser reçoit l'index I, exécute la même fonction polynomiale, qu'elle a en mémoire (morte ou non volatile), détermine l'adresse AD, va chercher son contenu qui est le même contenu Kc que dans l'autre carte du fait que la zone de mémoire désignée est identique dans les deux cartes.

La carte à personnaliser comporte par ailleurs un programme de décryptage $D^{-1}()$ qui est l'inverse du programme de cryptage $D()$ et qui permet donc de retrouver Kd en utilisant la même clé Kc qui a servi à crypter Kd.

Autrement dit, si $U = D(Kd, Kc)$, alors $Kd = D^{-1}(U, Kc)$.

La clé diversifiée Kd est donc retrouvée, et stockée dans la mémoire non volatile de la carte à personnaliser (zone inaccessible, c'est-à-dire ne pouvant pas être utilisée autrement que par le microprocesseur pour les besoins des fonctions de cryptage).

La clé diversifiée Kd peut également être stockée dans la mémoire de la carte maîtresse CM.

Seul a transité en clair entre les deux cartes l'index I. Celui-ci représente non pas un cryptage réel mais une dissimulation de l'adresse AD.

Mais même si un fraudeur arrivait à connaître l'adresse AD qui a servi au moment du cryptage, il faut comprendre que

- d'une part, le fraudeur ne connaît pas le contenu du fichier (inaccessible) qui est utilisé comme réserve de clés;

- d'autre part, l'index et donc l'adresse AD sont renouvelés à chaque fois d'une manière aléatoire et par conséquent l'observation d'une transmission ne permet pas de déduire des enseignements pour une prochaine fois.

11

La figure 3 rappelle les principales étapes de ces opérations.

On pourrait envisager d'utiliser comme mémoire commune aux deux cartes non pas la mémoire morte de programme de système de la carte mais une mémoire
5 électriquement programmable (non accessible en écriture effacement ou lecture) pourvu qu'elle ait un contenu identique pour les deux cartes.

La clé de cryptage Kc trouvée à l'adresse AD peut
10 être constituée par un mot à cette adresse, ou plusieurs mots consécutifs débutant à l'adresse AD, ou encore une fraction du mot à l'adresse AD. On peut aussi envisager des solutions plus complexes de choix de la clé à partir de l'adresse AD : par exemple, la clé peut être
15 constituée par le premier bit de x mots successifs à partir de l'adresse AD.

REVENDEICATIONS

1. Procédé de transmission cryptée d'une information (Kd) entre deux cartes à microprocesseur (CM, CP) qui ont chacune un fichier de mémoire (120, 220) à plusieurs adresses, ce fichier ayant un contenu
5 identique pour les deux cartes, procédé dans lequel on crypte l'information dans la première carte, on transmet l'information cryptée de la première carte à la deuxième, et on décrypte l'information dans la deuxième carte, ce procédé étant caractérisé en ce que le
10 cryptage et le décryptage sont effectués avec pour clé (Kc) le contenu d'une partie seulement du fichier de mémoire, identifiée par une donnée d'adressage (I) commune qui est utilisée par la première carte et transmise à la deuxième carte.
- 15 2. Procédé de transmission cryptée selon la revendication 1, caractérisé en ce que les cartes sont des cartes à microprocesseur comportant une mémoire morte de programmes dont le contenu est notamment un système d'exploitation de la carte, et en ce que le
20 fichier de mémoire commun utilisé comme réserve de clés de cryptage est la mémoire morte de chacune des cartes.
3. Procédé selon l'une des revendications 1 et 2, caractérisé en ce que la donnée d'adressage transmise de à la deuxième carte est un index (I) permettant de
25 calculer une adresse (AD), et en ce que les deux cartes comportent en mémoire un même programme de calcul P(I) pour calculer une adresse à partir de l'index.
4. Procédé selon la revendication 3, caractérisé en ce que l'index est élaboré dans la première carte.
- 30 5. Procédé selon l'une des revendications 3 et 4,

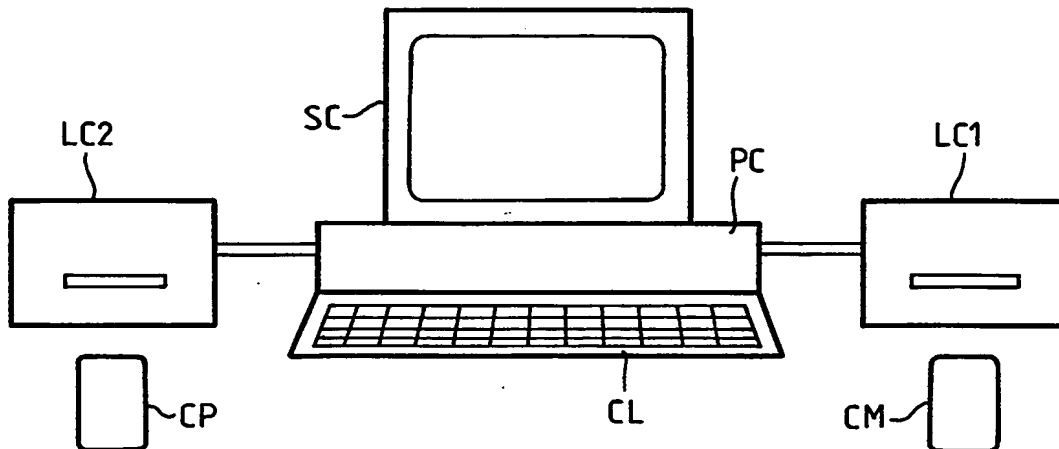
caractérisé en ce que l'index est élaboré de manière aléatoire, par un générateur pseudo-aléatoire ou un programme de calcul d'un nombre aléatoire.

6. Procédé selon l'une des revendications 3 à 5, caractérisé en ce que l'adresse est calculée par une fonction polynomiale à partir de l'index.

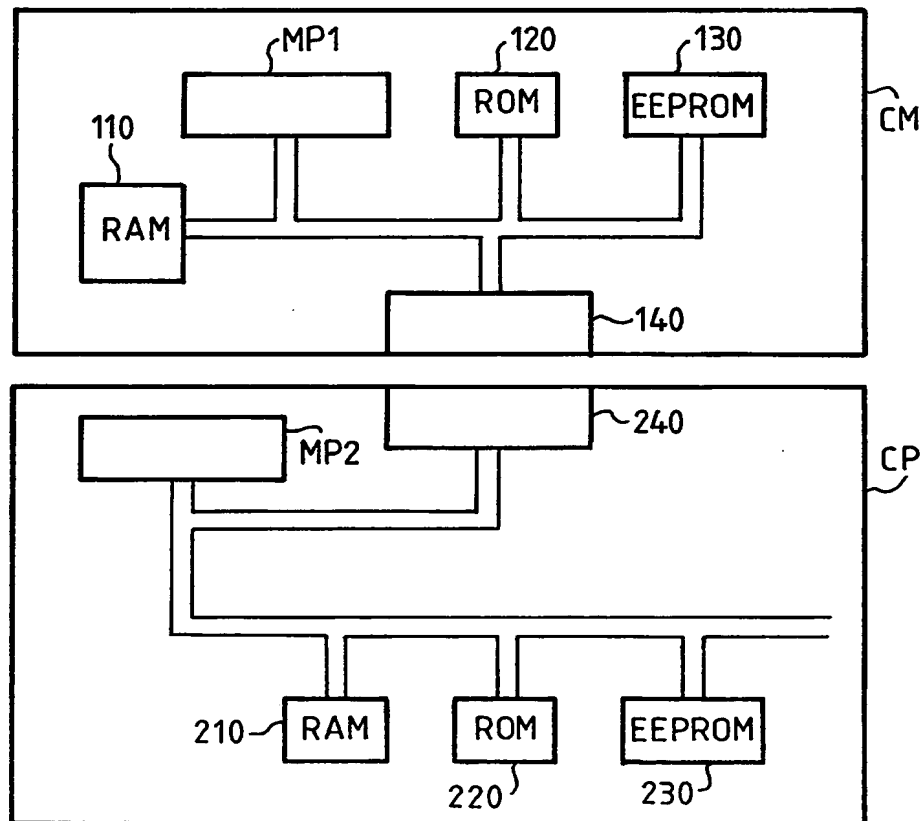
7. Procédé selon l'une des revendications précédentes, caractérisé en ce que la première carte est une carte de calcul d'une clé de cryptage diversifiée (Kd), cette clé étant destinée à être stockée dans la deuxième carte qui est une carte à personnaliser, en ce que l'information à transmettre est cette clé (Kd), et en ce que la première carte envoie à la deuxième à la fois la donnée d'adressage (I) et la clé diversifiée cryptée par une clé (Kc) trouvée dans le fichier de mémoire à partir de la donnée d'adressage.

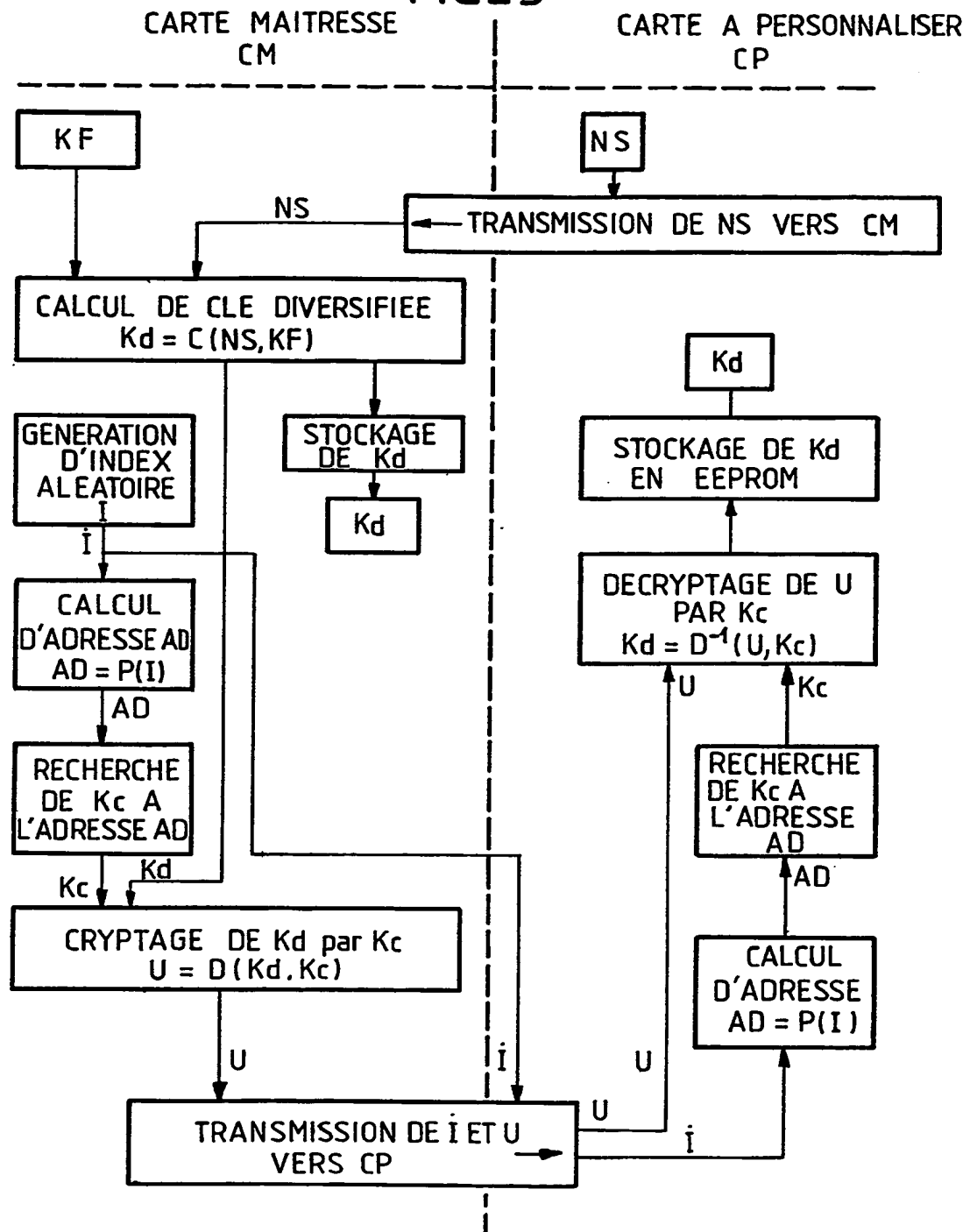
1/2

FIG_1



FIG_2



2/2
FIG. 3

REPUBLIQUE FRANÇAISE

2681165

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE
établi sur la base des dernières revendications
déposées avant le commencement de la recherche

N° d'enregistrement
national

FR 9111009
FA 462411

| DOCUMENTS CONSIDERES COMME PERTINENTS | | Revendications concernées de la demande examinée |
|--|--|---|
| Catégorie | Citation du document avec indication, en cas de besoin, des parties pertinentes | |
| Y | EP-A-0 035 448 (CII-HB) * abrégé; revendications; figure 1 * * page 8, ligne 33 - page 9, ligne 25 * | 1,2,7 |
| A | — | 3-5 |
| Y | EP-A-0 253 722 (BULL CP8) * abrégé; revendications; figures * | 1,2,7 |
| A | US-A-4 731 840 (S.M. MNISZEWSKI) * abrégé; figures * * colonne 3, ligne 44 - colonne 5, ligne 14 * | 1-5,7 |
| A | WO-A-8 503 787 (P. WHITE) * abrégé; revendications; figures * | 1-5,7 |
| A | FR-A-2 600 190 (BULL CP8) | |
| A | EP-A-0 096 599 (CII-HB) | |
| A | EP-A-0 284 133 (T.R.T.) | |
| | | DOMAINES TECHNIQUES RECHERCHES (Int. CL5) |
| | | G07F H04L |
| Date d'achèvement de la recherche 02 JUIN 1992 | | Examinateur DAVID J.Y.H. |
| <p>CATEGORIE DES DOCUMENTS CITES</p> <p>X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général O : divulgation non-écrite P : document intercalaire</p> <p>T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant</p> | | |